Opening Statement

September 16, 2011

Media Contact: Shane Wolfe

(202) 226-8417

Statement of Chairman Michael McCaul (R-TX)
Subcommittee on Oversight, Investigations, and Management

"Ten Years After 9/11: Assessing Airport Security and Preventing a
Future Terrorist Attack"

September 16, 2011
Remarks as Prepared

The morning of September 11, 2001, I remember watching television with one of my daughters and she asked "why did that plane fly into the building?" It was the second plane flying into the World Trade Center and at that point we knew it was no accident. America was under attack.

There were a total of 2,996 deaths that day. It is estimated US stocks lost $1.4 trillion in value. The United States went to war and we have lost thousands of men and women in the battle against terrorism. And we continue to fight the terrorists and protect our homeland.

The terrorists began this war by using our airports as launch pads. Over a period of ten years we have spent billions of dollars to mitigate such a threat. However, the 9/11 Commission's tenth anniversary report card concludes "…we are still vulnerable to aviation security threats." Specifically the report states we need to improve screening at airport checkpoints using biometrics and standardize identification documents to make it more difficult to circumvent security.

Additionally the attempted terrorist bombing of Northwest flight 253 on approach to Detroit on Christmas Day 2009, provided a vivid reminder commercial aviation remains an attractive terrorist target and underscores the need for effective airport security. Our major airports now have multiple layers of security.

Today's hearing will examine two of those layers; airport perimeter security, as well as new security measures being tested here at Logan International Airport in Boston. This airport has led the nation in new techniques and innovative methods to prevent another 9/11 attack.

Methods used by airports to control access vary because of differences in the design and layout, but all access controls must meet minimum performance standards established by The Transportation Security Administration.

TSA requires airports to control access using methods such as pedestrian and vehicle gates, keypad access codes with personal identification numbers, magnetic stripe cards and readers, turnstiles, locks and keys, and security personnel.

The Government Accountability Office 2009 report concludes there have been thousands of security breaches at airports around the country.

Additionally, it has been reported a young man breached perimeter security at Charlotte/Douglas International Airport and hid in the wheel well of a passenger plane. His body was found along Boston airport's flight path. Department of Homeland Security Secretary Napolitano said, "Clearly if somebody, a 16-year-old, is able to circumvent standards and requirements and get into the wheel well of a plane, there has been a breakdown."

Although some of these breaches are accidental, some may represent dry runs by terrorists.

The GAO examined airport perimeter security and concluded that TSA should develop a comprehensive risk assessment of airport security, and milestones for its completion; an evaluation plan for any future airport security pilot programs; and a national strategy for airport security that includes key characteristics, such as goals and priorities.

Not only is perimeter security of special concern, but passenger screening is essential if we are to prevent another 9/11.

TSA employees perform approximately 1.8 million screens a day, 2 million on holidays and have screened more than 6 billion travelers since September 2001.

The methodology has not always been perfect. And the sheer magnitude of this effort is certain to garner critics about the procedures.

TSA is attempting to improve security by testing a new program designed to identify potentially dangerous passengers before they board aircraft. The Screening Passengers by Observation Technique (SPOT) originated at Boston Logan airport in 2003. SPOT is designed to utilize non-intrusive behavior observation and analysis to identify high-risk passengers who may be a threat.

The Behavior Detection Program, a modification of SPOT, will have specially trained agents question passengers and gauge their reaction before they board aircraft. Based on physical clues or answers to questions, these officers should be able to detect suspicious behavior. The analysis will help determine if a passenger should go through additional screening. The program is based in part on the Israeli model of passenger screening. The GAO has examined this program and concludes it should be fully validated before it is used in airports throughout the United States.

I hope I never have to answer a question from my daughter again about planes flying into a building because of a terrorist attack.

We are here today to make sure security is in place to prevent such questions and another tragedy.

One final note; I would like to thank the Massachusetts Port Authority for hosting this hearing, all the witnesses present and especially my friend and colleague, Congressman Bill Keating for his insights about aviation security.

With that I recognize the Ranking Member of the Subcommittee, the gentleman from Massachusetts, Mr. Keating, for five minutes for the purpose of making an opening statement.